HOME CARE
AUTOMATION REPORT

Vol. 10 No. 7 ★ July 2005 *from Stony Hill Publishing*

State Legislators Begin to Respond to Security Crisis

Business as usual for the Feds however

Amid growing public concern about identity theft, already this year nearly a dozen states have passed legislation responding to the recent rash of security incidents reported by companies such as ChoicePoint, LexisNexis and Bank of America. More than 20 additional states are considering similar legislation. States that have passed new security laws include some of the nation's largest (Florida, Texas, Illinois, New Jersey) and some of the smallest (Maine, Montana, North Dakota).

While state legislators have reacted quickly to what the popular press is characterizing as an "identity theft crisis," it is business as usual in Washington DC, where the wheels are turning slowly and securing personal information is being turned into a partisan issue. A variety of bills have been introduced in both the House and Senate, with the most vocal proponents for action found on the Democratic side of the aisle. To date, Senate Judiciary Committee

Continued on page 3

Sorting Out New Breeds of Mobile Computers, PDAs

New choices include lighter weight, better screens

One sign that a technology has come of age is that user discussion turns from "do we need one?" to "which one do we want?" Broader acceptance of a technology tool increases familiarity with detail, which in turn leads to rising user sophistication and finer-tuned choices. Once the novelty of the horseless carriage wears off, the black Model T gives way to an endless array of features and colors. The same threshold is currently being crossed by clinicians with respect to mobile computers and PDAs.

Point-of-care computing has been around in home care since the late 1980's and began to gain an industry foothold in the mid-1990's. The technology experienced a surge as Medicare-certified agencies that survived IPS healed their financial wounds and began to recover under PPS. Today, home care software vendor account representatives agree, it is difficult if not impossible to compete without a POC module to offer.

Continued on page 5

Inside This Issue

CMS Announces National Provider Identifier Instructions

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) call for adoption of standard unique identifiers for health care providers and health plans. Last month, CMS revealed its plans for the National Plan and Provider Enumeration System (NPPES) along with its implementation timetable for use of the National Provider Identifier (NPI).

Note these dates

Transition to NPI will be gradual, taking place over the next two years.

- Now through January 2, 2006: use existing, legacy Medicare numbers. Claims with only new NPI numbers will be rejected.
- January 3, 2006 through October 1, 2006: use legacy Medicare number or both legacy and NPI numbers. Intermediary systems will accept legacy Medicare numbers alone *and* they will accept NPI numbers accompanied by existing legacy Medicare numbers but they will not accept NPI numbers alone.
- October 2, 2006 through May 22, 2007: use either number. Systems will accept an existing legacy Medicare number alone, an NPI number alone or both together. CMS says this overlap period will allow six to seven months of provider testing before legacy Medicare numbers are no longer accepted.
- May 23, 2007 and beyond: CMS intermediary systems will only accept claims with NPI numbers.

What you have to do

To be assigned an NPI number, providers will need to complete a 6-page NPI application form and submit it to CMS. The PDF format application can be downloaded from http://www.cms.hhs.gov/forms/cms10114.pdf. Further information, including educational tools, is available at a special CMS implementation web site: https://nppes.cms.hhs.gov.

Does everybody have to have an NPI?

Every provider must have an NPI and many will apparently have to apply for multiple identifiers. From the NPPES web site Frequently Asked Questions:

> "All providers conducting electronic transactions will be required to comply with these standards. Each organization subpart or physical location that is State-certified or licensed as a health care provider will be considered a health care provider in its own right and must apply for and will be assigned an NPI. Each physical location of a supplier of DME, orthotics, prosthetics, or supplies will be considered a health care provider in its own right and must apply for and will be assigned an NPI."

Follow Up: PGBA Problems Cause Delays for Other RHHIs

We reported last month that a recent software upgrade at Palmetto Government Benefits Administrators (PGBA) disabled the intermediary's claims processing for two weeks, causing more than a little distress among providers in the Southeast region served by the South Carolina-based RHHI. As a result, CMS has decided to delay similar upgrades at other intermediaries until PGBA analyzes the problem's source.

The culprit is called Healthcare Integrated General Ledger Accounting System (HIGLAS). It performs intermediaries' accounting and general ledger processing, supposedly better than the system it replaces, the Fiscal Intermediary Standard System (FISS), which will continue to be used for claims processing. HIGLAS was supposed to have had no impact on claims but something – no one is saying what – went wrong with the PGBA implementation, causing it to shut down claims processing entirely. On orders from CMS, PGBA staff spent the Memorial Day weekend handwriting checks and sending them out by FedEx.

Cahaba, UGS and AHSMedicare (Maine) were scheduled to implement HIGLAS in stages through late 2005 and early 2006. Providers that submit claims to one of these three intermediaries do not need to panic, however, as CMS has done that for them. HIGLAS is on indefinite hold, we were told by Cahaba spokesperson Susan Jesse Pennington.

Cahaba was supposed to transition to HIGLAS during the latter half of FY 2005, meaning before the end of September. UGS and AHSMedicare had not yet been told when to expect HIGLAS conversion but knew it would be well into FY 2006. Now it looks like CMS is making no implementation commitments any time through the end of that fiscal year either.

States Pass Security Laws continued from page 1

Chairman Arlen Specter (R-PA) is the only Republican to put his name on proposed legislation.

California as role model

Most legislation already enacted or still being considered by states, as well as proposals being floated in Washington, is modeled, at least in part, after California's ground-breaking security breach disclosure law that went into effect almost two years ago. It is the California law that has brought to light the latest rash of security incidents. Without it, quite frankly, the country would be going about its e-business as usual and it is not likely that Newsweek would make the growing threat of identity theft their July 4 cover story.

In summary, the California law applies to any entity that stores personal information on California residents electronically. Should a business experience a security breach that may include data on California residents, it is required to notify the affected individuals. Further, if the breach affects a large number of individuals, the media must be notified.

ChoicePoint was the first security breach to be widely publicized outside of California, although there were dozens more in-state incidents that preceded the Atlanta company's February disclosure. Earlier incidents, in fact, included a huge breach at UC-Berkeley that potentially compromised personal information on 1.4 million home care patients and caregivers (see HCAR, November 2004). Since ChoicePoint went public, nearly two dozen security incidents have come to light, impacting more than 50 million individuals.

The States' reaction

In what almost appears to be a game of "one-upmanship" an array of security solutions are coming from the states. State's Attorneys General and Governors are competing with each other to see who can get the "toughest" security law on the books the fastest. All appear to be trying to capitalize on the public's growing security concerns.

While the California model is being used as a framework for most state proposals, several pieces of legislation that have already passed may provide an indication of things to come. Here are some key state examples.

Florida: HB 481, signed by Governor Jeb Bush on June 16, is the toughest of the bunch. It includes notification requirements much like California's, but expands coverage to include third-parties that may have data on Florida residents (e.g., benchmarking firms, software vendors). Penalties for failure to notify can be as much as $500,000 and affected individuals can sue to recover damages. The Florida law went into effect on July 1.

New Jersey: AB 4001 was passed by the New Jersey legislature in mid-June and should become effective late this year. This bill is being heralded by privacy advocates as one of the best to be passed thus far. It includes notification provisions that apply to all businesses and to third-parties. It also requires notification of the state police before contacting affected individuals.

Illinois: With much fanfare, Illinois Governor Rod Baglojevich signed HB 1633 into law on June 16, proclaiming that the new law would provide consumers "some peace of mind" with regard to identity theft. The Illinois law requires timely notification of affected parties. In an interesting twist, companies that fail to provide notice can be prosecuted under the state's Consumer Fraud and Deceptive Business Practices Act.

For a complete listing of security breach legislation enacted or being considered on a state-by-state basis, consider visiting the National Conference of State Legislatures website at http://www.ncsl.org/programs/lis/CIP/priv/breach.htm. This site includes links to specific legislation and is periodically updated so you will be able to keep up with developments in your state.

Ripple effects

One of the features of both Florida's and New Jersey's legislation that is likely to be emulated in other states is the extension of liability to third parties that store or process personal information on state residents. Software vendors that remotely host applications, benchmarking firms that routinely exchange patient data and other companies that periodically access agency systems will now be exposed to potential litigation. These organizations must notify their business partners and ultimately state residents should they have a security incident.

The HIPAA Security Rule includes requirements for agencies and their business associates, and stipulates specific conditions that need to be incorporated into agreements with regard to electronic patient health information. Among these is a requirement to notify agencies when patient data may be compromised.

Continued on page 4

States Pass Security Laws continued from page 3

The new Florida statute ups the ante, not only requiring notification but imposing significant penalties and opening third-parties to potential suit.

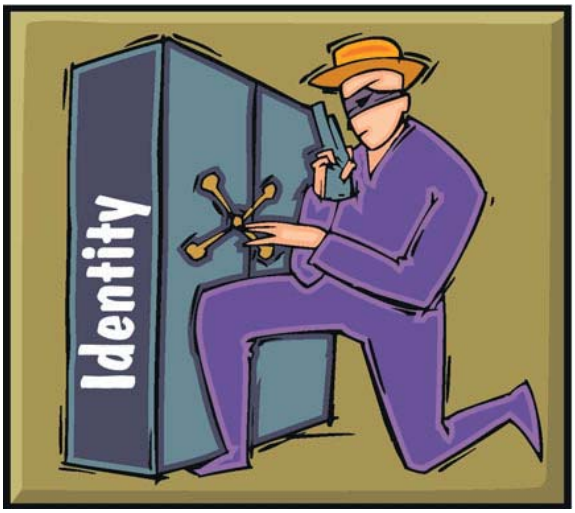
In spite of their "state resident" focus, these laws will likely impact organizations beyond a given state's boundaries. The annual migration of "snowbirds" each fall and spring to/from states like Florida, Arizona and Texas will subject businesses throughout the U.S. to these new laws. This, in turn, will raise the specter of ChoicePoint-like notification should a security incident occur, for even small organizations.

Organizations doing business across the country, such as multi-state home care providers, will struggle with inconsistent and sometimes conflicting state laws. This is an issue being raised at a national level and in fact is becoming one of the primary drivers behind calls for a national security breach disclosure law.

Home care impact may be huge

Among those hardest hit by various security breach notification procedures that states are adopting will be healthcare providers, who already must comply with the federal government's HIPAA Security Rule that went into effect just a few months ago. Providers face a particular challenge following passage of these laws, which generally apply to all businesses that retain personal data on state residents. Unlike retailers and many other types of businesses, however, should a security breach occur, healthcare providers have a standard by which their security practices will be judged – HIPAA. Failure to comply with the Security Rule's requirements will most likely expose them to significant state litigation risk should they experience a security incident.

Home care's exposure in this new world of disclosure could be huge, according to HCAR publisher Tom Williams. His company, Stony Hill Management, conducted an e-mail survey of nearly 4,000 home care agencies, hospice and HME dealers that receive its weekly security bulletin. Williams reports that only 20% of home care providers indicated they are complying with the Security Rule. "We conducted our survey just days after the April 20th compliance deadline," he said, noting that nearly 200 organizations responded. "Because this is self-reported and is only from organizations that responded, I believe actual compliance is substantially lower." "Inability to find time to address the regulations" was the reason given for non-compliance by more than 90% of respondents.



This latter point should serve as a "red flag" for home care providers, according to Williams, as this spring DHHS published its HIPAA enforcement proposal. He explained that enforcement will be complaint-driven, but that the door remains open to on-site compliance reviews, most likely in conjunction with the survey process. "While DHHS is hoping to establish a collaborative approach to complaint resolution, they have clearly stated that an affirmative defense will not be available to providers who 'willfully neglect' to comply with the regulations," he said. "Not finding the time is a clear demonstration of willful neglect and an excuse that is not likely to stand up should a provider find it necessary to defend its actions in court."

Williams asserts that the threat to home care and hospice providers from these new state laws is very real. In a security compliance survey conducted last fall in conjunction with introduction of his company's *GetHIP-Security* software, providers were asked if they had ever experienced a security incident that compromised patient data. "One in six respondents (nearly 400 agencies) told us that they had experienced such an incident in the past," he reported. "The likelihood of an incident requiring public disclosure and exposing these organizations to potential litigation is significant."

Home care providers need to be particularly sensitive to the ramifications of not taking security seriously. "Home care is a referral-driven business, and executives need to think about how their referral sources and patients would react to disclosure of a security breach," Williams commented. For agencies in markets where there is significant competition for referrals, the ramifications could be devastating. "Put yourself in the shoes of a referring physician" he suggests. "Given an alternative to refer patients to a provider who had just publicly declared it had a security breach or one that had not, the decision seems pretty obvious."

Selecting Notebooks and PDAs continued from page 1

While POC software is kept current indefinitely through periodic upgrades, the hardware on which it operates has at best a three-year lifespan. Consequently, many experienced agencies are already into a second, or even third, round of laptop/ notebook computer or handheld PDA purchases. Where, previously, selection decisions tended to focus on selecting a vendor and its application, today's experienced POC users have also learned to become choosy about devices. Weight, screen size, battery life and durability are all factors now considered, not merely whether a particular device can run the vendor's application.

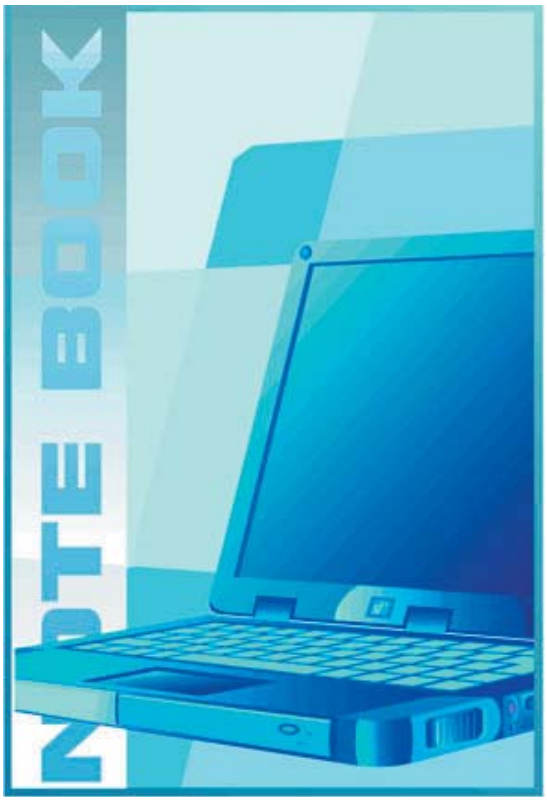
In response to increasing industry awareness of differences among hardware manufacturers and their alphabet soup of mobile models, we decided to see whether there is a consensus regarding the "best " home care computer or PDA. Our sources include home care agencies, vendors and published product reviews.

W/INTEL COMPUTERS

Taking your desktop on the road

Mobile computers driven by Intel, AMD or like-class processors that run current Windows Operating System versions are nearly equivalent to desktop computers in speed, function and storage capacity. Though home care has long referred to these machines as "laptop" computers, there are actually two distinct mobile categories. The big, heavy laptop is really only portable through an eight-hour work day if you are a linebacker, a California governor or use a wheeled computer case. What most home care nurses and therapists use today is the smaller, lighter "notebook" computer, or its even smaller cousin, the "ultraportable" notebook.

Software vendors always provide minimum configuration specifications for computers required to run their applications, and their suggestions should be an agency's primary guide. A good minimum configuration in most environments, however, would be a Pentium Centrino-M (or AMD AthlonT XP-M) ultra-low voltage processor running at 1Ghz, at least 256MB of memory, a 12-inch display, wired and wireless networking, Microsoft Windows XP, a 20 GB hard drive and an extra battery or car charger. M-series processors use less battery and produce less heat; they are



slower but still fast enough for most home care POC applications.

Traditionally, all computers are obsolete the day they arrive on store shelves. The advent of 64-bit processors is the latest cause of that phenomenon. It is a significant cause, however. Once AMD Turion 64 and Intel Xeon prices pass through the mandatory, new-release overpriced phase, they will begin to appear in affordable notebooks and change today's guidelines. Until then, they will be limited to use in high-end servers and multi-processor environments.

Human interface components such as keyboard size, screen clarity, touch screen functionality and touchpad comfort and ease of use are important considerations. It is wise to let those who will use the notebooks examine them, lift them and test these components before selection. Field clinicians typically do not require floppy or CD drives and have *no* need for writeable optical drives. If a model with a CD burner as standard equipment is suitable for all other reasons, the HIPAA-aware IT department will remove CD copying software or disable the drive before issuing notebooks to staff.

Many models come with external CD drives, which is an excellent compromise for two reasons. System weight is less for the user and technicians can still install software by attaching the drive as needed. If the external optical drive is optional, it is even better. You may want to reduce costs by purchasing one drive for several notebooks.

Price is not the only way to control cost. One agency we contacted managed to write a relatively creative clause into its hardware purchase contract. Initial price was discounted based on total number of notebooks ordered but delivery was taken in phases to coincide with the agency's gradual, branch-by-branch implementation schedule. Cash flow was eased and warranty clocks did not start ticking until each computer was delivered.

Continued on page 6

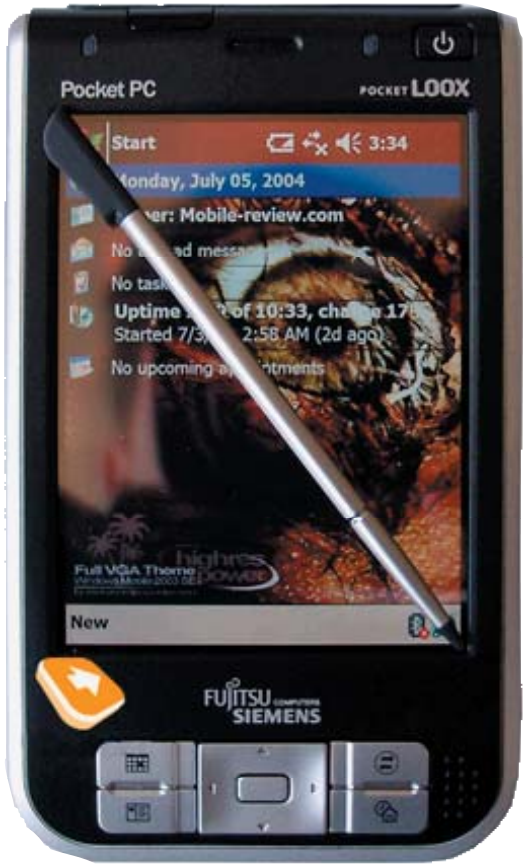
Selecting Notebooks and PDAs continued from page 5

In recent years, Fujitsu's *Lifebook* notebook series has dominated the home care POC market, though today there are several other choices in the category. The Panasonic *ToughBook* line is said by some agencies to be more durable, an important consideration in the abusive home care environment. As outlined in the chart on page 8, Acer, Averatec, Dell, HP, Panasonic, Sony and Toshiba offer units with similar features to the Fujitsu, though at wide-ranging prices. Naturally, however, price cannot be the only consideration. Service and support, when they fail, can quickly make cost savings a distant memory and are likely to have a negative effect on employee morale.

The Fujitsu *T4010D* seems to be the current favorite among agencies experienced at POC automation. According to Jim White of Misys, users appreciate the ability to chart quickly with a stylus on its touch screen. White says his customers have commented that handwriting recognition is greatly improved by Windows XP Service Pack 2. "It translates even the worst chicken scratching after just a short learning period," White said. "We can collect patient signatures on the Fujitsu now; one less piece of paper to handle."

PALM AND POCKET PCs

More than a half dozen software vendors offer Palm OS or Pocket PC devices as an option or as their only point-of-care choice, including CareCentric, Golden Rule Software, Healthcare Automation, HealthWyse, Homecare Homebase, InfoSys, McKesson and Misys. Healthcare Synergy and RiverSoft offer PDA-based POC through interfaces with Golden Rule and Healthcare Synergy also offers a device from Global Reliance Associates. In spite of early doubts about carrying a limited-function handheld device instead of a full computer into the field, there is no shortage of examples where one of these companies replaced a notebook-based POC vendor when winning a new customer.



Generally, vendors that offer primarily notebook point-of-care systems have added a PDA option with a software application customized for specific employees such as LPNs, home health aides or contract therapists. Vendors that offer only PDAs make all functions available, from scheduling to OASIS assessments, daily visit notes and medication databases. As with all generalizations, there are exceptions.

With the introduction of VGA displays, the argument about handheld computers being too difficult for "over-40" clinicians to read has been virtually eliminated. The initial Toshiba e800 was followed by mass release of Pocket PCs with VGA screens. Colors are sharp, lighting is more than adequate indoors and out and the increased pixel count eliminates some of the page changing during OASIS assessments that bothered some early PDA adopters.

Currently, Asus, Fujitsu/Siemens, Toshiba, HP (Compaq) and Dell offer VGA Pocket PCs, with more on the way. As with notebook computers, prices and features vary widely and caution is advised. These gadgets are attractive, relatively inexpensive and easy to overbuy. A necessary first step is to decide exactly which features are most likely to be used before starting your shopping, especially if accompanied by anyone from your IT department or a staffer wearing a Star Wars cap.

As with cell phones, marketing is aimed at young gamers and audiophiles. If your nurses are not going to play MP3 files between visits, don't pay for the feature. GPS capability may be a more practical luxury for a home care nurse but, at the top end, one feature generally comes with the other.

Resist fretting over an imperfect decision your first time around or regretting not having waited for an enhancement that became available three months after you placed an order. According to Steven Booth of HealthWyse, you'll get another chance soon enough. "We set the expectation that PDAs should be replaced every 2-3 years," he informed us. "The nature of this market is that the point-of-care device, whether it is a PDA or laptop, takes a real beating." Budget accordingly.

Continued on page 7

Selecting Notebooks and PDAs continued from page 6

Palm

According to Dean Craig of Golden Rule Software, the *Palm Tungsten E* has become the most popular choice among users of its *OasisPalm*™ point-of-care application. At under $200, it still has most of the features needed in home care. It is not VGA but its 320x320, full-color screen is still readable. 32MB of RAM is adequate for Golden Rule customers and the rechargeable Lithium Ion/Polymer battery easily lasts through an entire work day. As yet, palmOne, Inc., the company formed by the merger of Palm, Inc. and Handspring, does not offer a VGA display.

Pocket PC

The Wal-Mart of computer manufacturers, Dell is slowly but surely taking market share away from older Pocket PC makers with its *Axim 50* line. Golden Rule's Craig reported that it has become the device of choice among users of Golden Rule's new Pocket PC application. Steven Booth of HealthWyse concurs. "All of our new customers are going with the *Axim x50*," he told HCAR.

The *X50v* runs on an Intel "XScale™ 624MHz processor and features 64MB of SDRAM. The VGA version approaches $500 while the 240x320 screen starts about $200 less. GPS Navigation Systems add nearly $200 to either system, more if Bluetooth enabled. Protective carrying cases and virus software, both necessities in this environment, add a one-time $25 charge and a $35 annual subscription fee, respectively.

Fujitsu-Siemens and HP also offer useful lines for budget-conscious agencies. The Fujitsu *Pocket LOOX 410* and *420* are QVGA displays at 240x320 pixels resolution in the $400 range. The *LOOX 710* and *720* offer VGA but run a couple hundred dollars more. The higher end units also come standard with WiFi, Bluetooth, a camera and infrared.

HP's entry is the *iPAQ hx4705* at around $600 with VGA and the QVGA *hx2415* at $400. The reason for the similarities among Dell, Fujitsu and HP is that all are manufactured by the same Taiwanese company, Microsoft hardware platform development partner HTC.

For a brief feature comparison, refer to the chart on page 8.

HIPAA Security Tool Available

Stony Hill Management, publishers of HCAR, has reported that its GetHIP software is already in use at more than 1,000 locations throughout the U.S., making it home care's most widely used HIPAA compliance tool. *GetHIP-Security* is designed to help home healthcare providers comply with the HIPAA Security Rule, which went into effect in April. The software is highly scalable, with users ranging in size from more than 200 sites to single-site providers with as few as three computers. A version of *GetHIP-Security* is also available for long-term care and assisted living facilities.

GetHIP-Security is the third in a series of HIPAA compliance tools developed by Stony Hill Management. In 2003, more than 500 organizations utilized *GetHIP-Privacy* to achieve compliance with federal privacy requirements, and thousands of staff were trained using the company's HIPAA educational videos.

GetHIP-Security users give the product consistently high marks for comprehensiveness and ease-of-use. The software employs a TurboTax™-like interface, with users responding to a series of questions about their organization's operations and security measures. They are guided through a thorough assessment by the software's unique "HIP Advisor" feature, an in-house consultant that provides implementation advice and step-by-step explanations of regulatory requirements and key security concepts. As users respond to questions, the software automatically builds a work plan, presents sample documents and provides a variety of tools to document and manage compliance efforts.

GetHIP-Security can be installed on a single PC or deployed over a network, and an enterprise version is available for larger providers. A single-site, perpetual software license is $750, with significant discounts available for multi-site organizations. Six months of support and maintenance are included in the initial purchase price. Ordering information is available at www.hipaahomecare.com or by calling 866-436-7047. An evaluation copy of the software can be downloaded from www.gethipsoftware.com/evaldownload.

A Comparison of Popular Windows Ultraportable Notebook PCs

BRAND/MODEL	CPU	RAM INSTALLED/ MAX	HARD DRIVE INSTALLED/MAX	DISPLAY / MAX RES.	WEIGHT & DIMENSIONS	OTHER	WARRANTY	PRICE RANGE
ACER TRAVELMATE 3002WTCi	Intel Centrino Pentium M, 1.73 GHz	512MB – 2GB	60GB IDE	12.1" 1280x800	3.6 lbs. 11.7" x 8.3" x 1.3"	Ext. CD RW, 3 USB ports WinXP Pro	1 year	$1229-1600
DELL LATITUDE D410	Intel Centrino Pentium M, 1.6GHz	256MB – 2GB	30GB IDE	12.1" 1024x768	4.9 lbs. 10.9" x 9.4" x 1.3"	Int. CD-ROM WinXP Home	3 years	$1209
FUJITSU LIFEBOOK P7010D	Intel Celeron M, 1 GHz	256MB – 512MB	40-80GB IDE	10.6" 1280 x 768	3.3 lbs. 10.5" x 7.8" x 1.4"	Int. CD R/W, Fingerprint, WinXP Home	1 year	$1349-2099
HP COMPAQ nc4000	Intel Centrino Pentium M, 1.4GHz	256MB – 1GB	40GB IDE	12.1" 1024 x 768	3.5 lbs. 11" x 9.2" x 1.1"	No CD Battery 3 hrs. WinXP Pro	3 years	$1000-1349
PANASONIC TOUGHBOOK T2	Intel Centrino Pentium M, 1.2 GHz	256MB – 512MB	40 GB IDE	12.1" 1024x768	2.6 lbs. 10.6" x 8.3" x 1.3"	Battery 3 hrs. WinXP Pro	3 years	$2188-2499
SONY VAIO TR Series	Intel Centrino Pentium M, 1 GHz	512MB – 1GB	40 GB IDE	10.6" 1280 x 768	3.1 lbs. 10.6" x 7.4" x 1.5"	Int. CD R/W Battery 7 hrs. WinXP Home	1 year	$1500-2200
TOSHIBA LIBRETTO U100	Intel Centrino Pentium M, 1.2 GHz	512MB – 1280MB	60 GB IDE	7.2" 1280 x 768	2.2 lbs. 8.3" x 5.7" x 1.2"	Bluetooth, Fingerprint, WinXP Pro	3 years	$1899-1959

All have fax/modems, network cards, wireless LAN, 1 or 2 USB ports, microphone and headphone jacks and CD drives. None have floppy drives. Typical battery life is 5 hours. Exceptions are noted.

A Comparison of Popular PDAs

BRAND/MODEL	CPU	RAM INSTALLED/ MAX	OPERATING SYSTEM	DISPLAY / MAX RES.	WEIGHT & DIMENSIONS	OTHER	WARRANTY	PRICE RANGE
ASUS MyPal A730 and A730W	Intel XScale PXA270 520MHz	128MB 1 CF slot 1 SD slot	Windows Mobile 2003 Second Edition	VGA	6 oz. 4.6" x 2.87" x .66"	Camera, Wireless, Bluetooth	1 year	$499-599
FUJITSU POCKET LOOX 720	Intel® PXA272 520MHz	128 MB plus 64 MB flash	Windows Mobile 2003 Second Edition	VGA	6 oz. 4.8" x 2.8" x .6"	Camera, Wireless, Bluetooth	1 year	$700
DELL AXIM X50	Intel XScale PXA270 520MHz	128MB plus 64MB SDRAM 1 CF, 1 SD slot	Windows Mobile 2003 Second Edition	VGA	6.2 oz. 2.9" x .7" x 4.7"	Wireless 802.11b, Bluetooth	1 year	$499
HP iPAQ hx4700	Intel Bulverde 624MHz	128 MB 1 CF slot 1 SD slot	Windows Mobile 2003 Second Edition	VGA	6.6 oz. 5.17" x 3.03" x .59"	Wireless 802.11b and Bluetooth	1 year	$578
TOSHIBA e830	Intel XScale 520MHz	128MB 1 CF slot 1 SD slot	Windows Mobile 2003 Second Edition	VGA	6.8 oz. 5.3" x 3.0" x 0.6"	Wireless 802.11b and Bluetooth	1 year	$499-599
PalmOne Tungsten E	TI TECH 126 MHz	32 MB 1 SD slot	Palm OS	320x320	4.6 oz. 4.5" x 3.1" x .5"	IrDA	90 days	$175

Email Accidents Prove Costly

Third-party email encryption systems require investment but going without them can be even more expensive. In a work environment where most staff has access to electronic protected health information (ePHI) and an unencrypted email system, even if privacy and security policies are in place, the potential for serious trouble looms large. A single careless or disgruntled employee can bring disaster to a company.

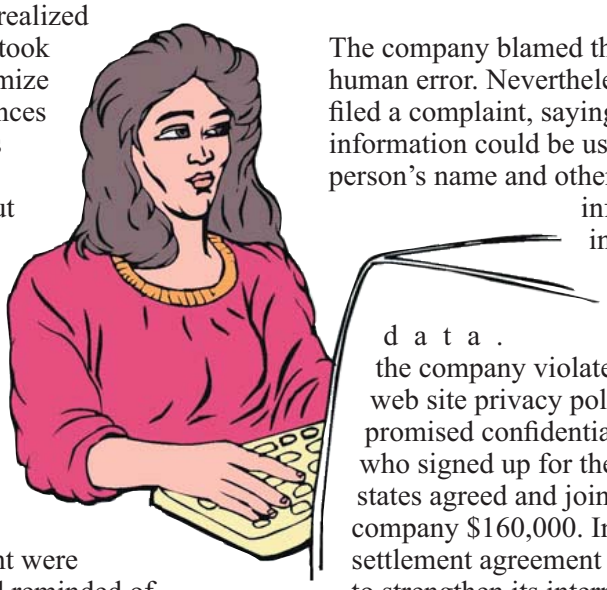
Just ask Eli Lilly, Kaiser Permanente and Florida's Palm Beach County Health Department. Following accidental email errors or malicious activity by a single individual at each organization, two of these three healthcare organizations have been assessed six-figure fines and the other is still pending.

In the earliest of these incidents, pharmaceutical manufacturer Eli Lilly paid $160,000 to New York, California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, and Vermont to settle a multi-state suit. The complaint, investigated by California and filed by New York State Attorney General Eliot Spitzer, alleged that names and email addresses of Prozac users had been exposed through sloppy emailing.

Former Kaiser Foundation Health Plan employee Elisa D. Cooper, whose blog handle is the "Diva of Disgruntled," found patient information on a publicly accessible section of the company's web site while researching material to dispute her termination. When complaints to her ex-employer were ignored, she reposted the offending page on her own web site until she got the attention of the Office of Civil Rights, which is charged with enforcing the HIPAA Privacy Rule. Just last month, Kaiser was fined $200,000 by the California Department of Managed Health Care (DMHC) for not taking action when they first learned about the error.

"Not only was this a grave security breach, but Kaiser did not actively work to protect patients until after they had been caught," said DMHC director Cindy Ehnes in a press release. "We're imposing this fine because we consider this act to be irresponsible and negligent at the expense of members' privacy and peace of mind."

In Palm Beach County last February, Florida Health Department statistician John Nolan accidentally attached a confidential list of the names of 6,500 HIV-positive persons to a routine email containing county HIV/AIDS statistics and addressed it to 800 other health department employees. Nolan immediately realized his error and took steps to minimize the consequences by getting his department's IT staff to shut down the network and purge all e-mail attachments. Ten employees who had already opened the attachment were contacted and reminded of their confidentiality agreements. It does not appear that the list made its way outside of the county's system.



It's a good thing. According to the *Palm Beach Post*, releasing protected medical information is a first-degree misdemeanor punishable by up to one year in prison in Florida. Though they are "99% sure" the information was contained, the county health department will launch a "full and major investigation," according to health department spokesperson Tim O'Connor. In addition, state health officials are launching an investigation into the issue at the behest of department Director Dr. Jean Malecki. Although Nolan might face disciplinary action, he likely will not be prosecuted because he "clearly didn't intend to release the list," O'Connor told the *Post*.

The Lilly situation was a little different. The Indianapolis company has privacy and security policies in place but somehow one customer service employee didn't get the word. The company invites Prozac users to sign up for automated email reminders to take their dose of the antidepressant. One day, that email went out with all 669 recipient addresses in the "To" field instead of the "Blind Copy" field. Everyone who received the reminder could ready everyone else's email address.

The company blamed the incident on human error. Nevertheless, the ACLU filed a complaint, saying email address information could be used to find a person's name and other personal information, including some medical history data. It said the company violated its own web site privacy policy, which promised confidentiality to those who signed up for the service. Eight states agreed and jointly fined the company $160,000. In addition, the settlement agreement requires Lilly to strengthen its internal standards relating to privacy protection, training, and monitoring. Lilly will also institute automated checks for any of its software that accesses consumer information databases. The settlement agreement did not, however, require that the company admit it broke any laws.

According to privacy attorney Stephen Wu of the InfoSec Law Group in Mountain View, California, new stories about security breaches appear in the headlines practically every week. In "Cisco Systems vs. Alcatel" a disgruntled employee sent samples of proprietary source code to prospective new employers, as if to say, "Look what I can bring with me to my new job." In a tobacco case, a legal aide

Continued on page 10

eMail Encryption continued from page 9

emailed an 80-page excerpt of a firm's formal trial plan to the other side's attorney, asking for a $2 million bribe for the complete plan.

It could happen to any organization
Such stories make headlines because they involve major corporations with recognizable names or government entities. One cannot extrapolate, however, that incidents like these *only* happen to big organizations. Headline-worthy gaffes are most useful as warnings to all. Each of the organizations involved in the above incidents had secure email systems and strict policies in place. Whether you have implemented PGP, SSL or 128-bit email encryption or have strict policies about what can and cannot be included in email communications, or both, it is always possible for someone to hit the wrong button.

What can be learned from these headline-grabbing examples is that the "oops" factor can result in fines that might be annoying to a large corporation. Less apparent is the impact such an error could have on a small company, potentially bringing it to its knees. The first thing OCR (enforcing HIPAA Privacy) and CMS (HIPAA Security) say they will look for after a privacy or security breach comes to light is whether the covered entity (home care agency) has made a good-faith effort to protect patient information. Consequences will be more severe for those providers that release patient information, even accidentally, if they can not demonstrate they have made a serious effort to secure such data.

Is email encryption required?
To understand how to proceed, InfoSec's Wu recommends becoming familiar with exact regulatory language before deciding whether to purchase encryption software. In paragraph 164.312(e)(1), the HIPAA Security Rule does not specify the purchase of an email encryption system but says covered entities must consider whether one is appropriate in their circumstances: *"[An agency] must, in accordance with 164.306... implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*

To understand whether this should be read as implying that email encryption is mandatory, the rule assigns two addressable specifications to this paragraph. One applies to Integrity Control, the requirement to assure that ePHI is not improperly modified without detection. The other, also an addressable specification, says, "Implement a mechanism to encrypt electronic protected health information *whenever deemed appropriate*. (emphasis added)

CMS commentary with the Security Rule explains that, when ePHI is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk. Organizations that connect to an ISP via dial-up modem, for example, incur little risk. Those with "always on" Internet connections run a much higher risk. Both, however, run equal risk with email. "Sending unencrypted email is akin to dropping a postcard in a mailbox," Wu emphasizes. "If you wouldn't send the results of someone's blood test on a postcard, don't send them via email either. Encrypted email, however, is more like inserting that post card into an opaque envelope."

CMS noted in its commentary that "…there are very few known breaches of security over dial-up lines and… nonjudicious use of encryption can adversely affect processing times and become both financially and technically burdensome." Elaborating on this concept, Security Rule commentary adds:

> Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear that there is not yet available a simple and interoperable solution to encrypting e-mail communications with patients. As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. *[Agencies] are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the Internet.* (emphasis added)

Throughout the Security Rule, CMS remains committed to the principle of technological neutrality, and does not specify a particular product or even algorithm strength, such as 128-bit encryption. The Rule's authors note that technology is constantly changing and that any specific recommendation would quickly be obsolete.

Addressing the addressable specification
None of this necessarily provides you clear direction for your specific organization. Attorney Wu adds some insight that might. "If an organization suffers an accidental or intentional release of ePHI through email or any other means, *reputation loss* will vastly exceed the cost of paying a fine or settlement," he said. "Dealing with breaches costs real dollars. Security planning by consent decree is no fun. Far worse, however, is the PR disaster, especially for referral-dependent businesses."

Wu's list of liability consequences included private civil suits, statutory claims of unfair and deceptive trade practices, common law negligence claims and government enforcement actions. "Telling patients you will keep their information private and then not doing so is sufficient to generate a deceptive trade practice suit," Wu said.

Continued on page 11

eMail Encryption continued from page 10

Full email encryption, complemented by strict corporate policies with clear consequences, may be all an organization can do to lower the risk of disclosure. However, as demonstrated by the Lilly, Kaiser and Palm Beach incidents, they cannot be 100% guarantors of prevention. Vigilance includes comprehensive and ongoing staff training and reminders, as well as a willingness on the part of management to demonstrate its commitment to its policies. Dr. John Halamka, CIO of Harvard Medical School, for example, claims that his organization fires "two or three doctors a year" over privacy policy violations.

Security consultant Steve Petermann represents a Georgia company, CipherTrust, which offers an email security appliance called "*IronMail*." He emphasizes the importance of protecting data and the network that houses it from *both* inbound and outbound email threats. "Spam will increase from 15 billion emails in 2000 to over 70 billion by 2007," he reported at a recent conference. "The *monthly* growth rate of phishing messages is 34% and over 80% of inbound enterprise email is undesired." In addition, he warns, inbound threats also include spoofing, denial of service attacks and hacker snooping.

Outbound threats, Petermann said, come under the heading of policy violations that open vulnerabilities to virus propagation, inappropriate content, IP address theft and regulatory violations. "According to the US Department of Justice, IP theft amounted to $250 billion in 2004," he continued. "Sexual harassment suits average $225,000, not including court costs. Regulatory compliance fines can be up to $250,000 per incident, not to mention possible jail time for executives."

Do not overlook IM

No discussion of email-based security challenges can exclude consideration of instant messaging, which is growing exponentially in the workplace. According to Andrew Burton of IMlogic, based in Waltham, Massachusetts, all businesses, not just healthcare providers, should implement an internal, corporate IM communications capability and forbid the use of public IM systems provided by Microsoft, Yahoo, AOL and the like. "IM is easier and more convenient than voice mail," Burton told an online audience recently, "and your employees are going to use it. Better that those messages should remain behind the company firewall rather than bounce all over the Internet before landing at a desk 50 feet from where they originated."

Private IM systems install easily onto standard desktops and networks and offer safeguards the public IM systems cannot. Encryption, user authentication and authorization, virus scanning, granular file controls, worm and malware blocking, anti-spam protection, internal message routing, client version controls and automatic security updates are typical of the threat protection and security offered by private IM systems. Compliance with regulatory requirements is also offered by message capture and permanent storage, compliance content filtering, log/audit/annotate capability, export to third-party systems and embedded legal disclaimers. Many systems also offer monitoring, reporting and message broadcasting.

Conclusion

The HIPAA Security Rule permits each organization to make its own decisions regarding how to best protect ePHI in transit. Commercial email encryption systems (see list at right) are probably necessary for medium and large providers, and are less important in small offices that may still communicate with modems instead of "always on" broadband connections.

Strict policies, including enforcement and consequences, are a must for all providers, regardless of size. Some policies may specify that patient information is never to be included in email messages and thereby skip the encryption question. Even under such a mandate, however, safeguards must be implemented against malicious incoming email.

Regardless of the path a home care provider or hospice selects to secure its patient information, its motivation *must* be to protect its patients, its business operations and its reputation.

Email Encryption Systems

As ID theft and security breach incidents continue to dominate the news, there is no shortage of available encryption technologies. An Internet search on "email encryption + healthcare + HIPAA" produces no fewer than 113,000 results. We'll narrow the list to a few companies we have encountered at recent tradeshows.

CipherTrust
Alpharetta, GA
http://www.ciphertrust.com

Encryption Solutions, Inc.
Santa Ana, CA
http://www.encryptionsolutions.net

IMlogic, Inc.
Waltham, MA
http://www.imlogic.com

Kryptiq Corporation
Beaverton, OR
http://www.kryptiq.com

MasterPrivacy.com
Thousand Oaks, CA
http://www.masterprivacy.com

Netilla Networks, Inc.
Somerset, NJ
http://www.netilla.com

Vericept Corporation
Englewood, CO
http://www.vericept.com

Zix Corporation
Dallas, TX
http://www.zixcorp.com

Tech Digest

NHIN making progress.
With nine years remaining to meet President Bush's goal to create a national health information network, progress can be seen on several loosely-related fronts.

- Senators Bill **Frist** (R-TN) and Hillary **Clinton** (D-NY) co-sponsored a bill, the **Health Technology to Enhance Quality Act of 2005**, that would provide $125 million per year in grants and loans to create Regional Health Information Organizations (RHIO).
- Senator Christopher **Dodd** (D-CT) introduced SB 1223 to provide a half billion dollars a year for health IT and a new executive-level officer to administer it and report directly to the President.
- In the House, Reps. Patrick **Kennedy**, (D-RI), and Tim **Murphy**, (R-PA), introduced the "21st Century Health Information Act" (H.R. 2234). This bill provides $50 million in grant funding to be spread among up to 20 different RHIOs.
- Last month, the House Appropriations Committee approved a bill for $75 million for the Office of the Health Information Coordinator, $58 million more than last year but $3 million less than the administration requested.
- HHS Secretary Michael **Leavitt** called for "organic cooperation" among providers, payers and technologists to come up with standards for exchanging data among disparate systems. He also created the "American Health Information Community" and announced he would chair it himself.
- The **Markle** Foundation, jointly with the Robert Wood **Johnson** Foundation, is providing $1.9 million to fund a project to "establish common policy values for sharing and protecting health data and then build the technical nomenclature and standards to support those policies. The project will begin with volunteer providers in Massachusetts, Indianapolis and Mendocino, California.
- Earlier this year, IBM announced it would build a test system to move health information, in this case dummy data, from one network to another.
- **CHIME**, the College of Healthcare Information Management Executives, sent a letter of support to Senators Frist and Clinton for their health technology bill.

VCs reveal hot investment targets.
At a recent **Dow Jones** conference, IT technology company executives and venture capitalists identified **security, enterprise data integration, health care and regulatory compliance** as some of the areas that will attract investment during the next few years. Describing the concept of "Service-Oriented Architecture," George Gilbert, of **Tech Strategy Partners**, a consulting and research firm focused on enterprise software and service, said, "We are going to see over the next five-plus years a very labor-intensive effort to get applications to talk to each other and liberate the data that's locked in disparate applications and databases."

Home care without the home.
A New England non-profit organization has started to send its street teams out to look for homeless people in need of medical care, armed with a BlackBerry strapped to their belts. **Boston Health Care for the Homeless** is testing e-prescribing in an environment where paper prescription forms often get lost. Mobile caregivers can send prescriptions to the nearest pharmacy from wherever they encounter a patient.

Has XP flopped?
A recent study makes a surprising discovery. After four years, Windows XP is installed in 38% of business PCs. Its predecessor, however, Windows 2000, maintains presence on 48% of corporate desktops. The study proves that Microsoft has a recurring problem: it has not provided sufficient justification – in features, performance or cost – for customers to give up older versions of software that's paid for and working just fine. If Gates and Company cannot move users to XP, how will it get them to open their wallets for Longhorn?

Vendor Watch

PtCT contracts marketing expert.
Atlanta-based **Patient Care Technologies** (PtCT) and home care marketing consultant, Michael Ferris of Chapel Hill, North Carolina, have teamed to provide marketing services to PtCT clients using the company's *well@home* home telehealth system. PtCT Sales VP Mark Hanna said the system has been opening referral source doors for providers and the company thought its customers could benefit from additional assistance developing creative marketing plans for this new technology.

Ferris has owned a home care company but most recently has been offering marketing consulting services through his company, **Home Care Marketing Solutions**. "I see [*well@home*] as an attractive value proposition for patients, families and community-based physicians and payers," Ferris said. "The need…is to get the word out."

The new service will provide *well@home* users with Ferris' sales and marketing training. Clients then have the option of supplementing the basic offering with additional, customized marketing consulting services. *well@home* was approved by the FDA in April, 2004.

Ferris is a featured speaker at national and state association meetings and conferences and the author of four books How To: Market and Deliver Legendary Service – Establishing the Gold Standard for Home Care, Managing Home Care Sales Teams for Legendary Results, 101 Home Care Promotional Strategies That Deliver Legendary Results Without Busting Your Budget and The Complete Guide to Home Care Sales & Marketing for Legendary Results.

http://www.ptct.com
http://www.hcmarketingsolutions.com

Continued on page 13

Vendor Watch continued from page 12

Homecare Homebase Introduces Mobile Customer Relationship Manager.
The *HCHB Customer Relationship Manager* is a new module for users of the **Homecare Homebase** Pocket PC-based point-of-care system, *Mobile Manager*. Released in late June, the CRM module gives agency marketing staff access to real-time referral volume, admission and discharge information on their PDA as it is uploaded to central servers from field clinicians. Also provided by the new module are customer call history, territory management tools, marketing reports and promotional programs.

The system tracks planned and completed marketing calls, suggests contacts in a similar geographic area, makes marketing staff aware of unsigned physician orders and provides information on marketing programs and initiatives developed by agency management. Built-in reports include marketing staff productivity, referral volumes and profitability by referral source. Managers may review calls completed, review expenses, examine performance measurements and update program information.
http://www.homecarehomebase.com

McKesson support site recognized.
The **Extended Care Solutions Group**, **McKesson's** Springfield, Missouri-based home care division, operates a customer-only "InfoCenter Web site" that has won recognition as one of the 2005 "Ten Best Web Support Sites" by the **Association of Support Professionals** (ASP). The site supports homecare, hospice and home telehealth systems users and is the first site operated by a hospice and homecare systems vendor to receive the award. The division finds itself in impressive company. Other 2005 winners include **Cisco Systems**, **Cognos and Microsoft**. Winners were selected by a panel of judges with expertise in Web support design and implementation. Criteria covered overall usability, design and navigation; knowledgebase and search implementation; interactive features; personalization and methodology used to address the major site development challenge.
http://www.horizonhomecare.com

"Most Wired" hospitals honored.
A study conducted by *Hospitals and Health Networks* magazine ranked the nation's hospitals on their use of technology to increase safety and quality, customer service, disaster readiness, business processes and workforce issues. Award winners will be announced at the **American Hospital Association's** July Leadership Summit. The **College of Healthcare Information Management Executives** (CHIME), a co-sponsor of the event, announced that 88% of this year's awarded organizations employ CIOs who are CHIME members. CHIME was formed to serve the professional development needs of healthcare CIOs and advocate more effective use of information management within healthcare.
http://www.hospitalconnect.com
http://www.cio-chime.org

Cerner to host health conference.
Kansas City-based **Cerner Corporation** has opened registration for its 2005 Cerner Health Conference, to be held October 9-12 at the Gaylord Palms Resort & Convention Center in Orlando. Keynote speakers will include HHS Secretary Michael Leavitt, CMS Administrator Mark McClellan and former Red Cross head Dr. Bernadine Healy. A number of educational sessions with a home care focus are planned, including regional Special Interest Group meetings.
http://www.cerner.com

Healthcare Automation looks west.
Rhode Island-based **Healthcare Automation, Inc.** (HAI) has established a distribution agreement with **Osion, LLC** of Bakersfield, California to market its home care and home infusion applications on the West Coast. Osion, led by long-time HAI customer Suzanne Schuler, has experience using *HomecareNet* and its predecessor product, *The I.V. Solution*, in Infusion, HME and home health care.
http://www.healthcare-automation.com

WEDI announces upcoming meetings.
The **Workgroup on Electronic Data Interchange**, an organization advising the government on HIPAA standards, has scheduled a series of meetings and conferences this summer and fall. Meetings are open to members and non-members. Details are available on the WEDI web site.

- **Claims Attachments Vendor Forum**, August 23-24, 2005, Hyatt Fair Lakes, Fair Lakes, VA.
- **WEDI NPI Industry Forum**, August 24-25, 2005, Hyatt Fair Lakes, Fair Lakes, VA.
- **WEDI Fall Conference**, November 14-17, 2005, Grand Hyatt Tampa, Tampa, FL.

http://www.wedi.org/public/calendar

Free Security Rule Seminar Available

Stony Hill Management, publishers of HCAR, has made its popular HIPAA Security Rule seminar available on the Web at no cost to home care, hospice, home infusion and HME providers. This seminar series is accessible from Stony Hill's website and includes four separate modules ranging in length from 30 to 40 minutes. A handout including slides accompanies each module.

Content, which includes audio, video and slides, is streamed over the Web. No special software is required to access and view the sessions but a high speed internet connection is recommended.

Over the last year, more than 4,000 executives have participated in Stony Hill's live Security Rule seminars and workshops. These sessions have been very well received across the country and attendees have consistently given them high marks. This four-part series is based on material used in these seminars and workshops. Topics covered include:

Part 1: Understanding Security Principles and HIPAA
Part 2: Risk Assessment and Initial Compliance Project Phases
Part 3: Administrative Safeguard Requirements
Part 4: Physical and Technical Safeguard Requirements

According to Stony Hill CEO Tom Williams, he is pleased with initial response to his seminar offer and is seeing traffic continue to build daily. "We began widely publicizing the seminar series in late March," Williams said, "and in a little more than a week more than 400 organizations registered. More than 50 different trade associations and vendors are working with us to let their members and customers know about our offer, so I expect this will continue for some time."

Williams recently announced that the seminar series would be available through August and noted that industry foot dragging on compliance will likely have him extending that time frame. "This feels much like the industry's reaction to OASIS several years ago," he said, explaining that many agencies took their time complying with that CMS initiative. "Home care providers will eventually get around to complying with this regulation. The increasing visibility of security incidents will ultimately bring them to the realization that this is a serious issue."

The free seminar series can be accessed by registering at Stony Hill's website, www.hipaahomecare.com.

WANT YOUR OWN SUBSCRIPTION?

If you got this copy of HCAR from someone else, you could have next month's issue delivered right to your email box as soon as it is published. Subscribing is easy. Just send us an email message with your name, organization and phone number. Make certain to put the words "new subscription" in the subject line. Or call us at **262-692-2270**. We'll send you the first issue absolutely free. If you like it, and we know you will, you can become a regular subscriber at our low introductory rate of $147 for 12 monthly issues ($110 off our regular price). *Special offer for association members!* If you belong to either a national or state association your first year e-subscription will be only $127. If you belong to both, there's an additional $20 savings, reducing your 12-month e-subscription price to $107. **That's more than 60% off our regular price.**

Publisher Tom Williams
Editor Tim Rowan
Page design Loran Mundy

Home Care Automation Report
is published monthly.
©2005 Stony Hill Publishing
ISSN 1083-5059

Our mission is to provide independent and timely information about how home health care executives use automation to boost productivity, cut costs and improve patient care.

Questions or comments?
Call Publisher, Tom Williams at
262-692-2270
Home Care Automation Report
Stony Hill Publishing
N5837 Kohler Rd., Fredonia WI
53021
e-mail info@stony-hill.com